Net-Centric Readiness for DoD Critical Mission Execution

Debra Tang
Chip Raymond

3/24/2006

LIFE CYCLE SOFTWARE ENGINEERING

Agenda

1. **Concepts of DoD Critical Missions Execution**
2. **Concepts of Net-Centric Readiness (NCR)**
3. **Global Information Grid (GIG) – ORD/CRD**
4. **Future Combat System (FCS) for NCR**
5. **Challenges for NCR**
6. **Countermeasures for the NCR Challenges**
7. **Conclusion**

Words from Subjects Matter Experts

" The two truly transforming things, conceivably, might be in information technology … and networking and connecting things in ways that they function totally differently …"

   -- Defense of Secretary Rumsfeld (8/2001)

" If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

   -- Sun Tzu (400 BC)

Principals for Winning Combat

➢ **Full Knowledge about Yourself and Adversaries**

  – **Information Superiority**

➢ **Enable Network for full Battle OP Tempo**

  – **Network Superiority**

➢ **Dominate the Full Spectrum of the Battlespace**

  – **Decision Superiority**

DoD Global Information Grid (GIG)
Joint Vision 2020

**Highlight the importance of Network-Centric Warfare (NCW) environment -- Enabled by the GIG**

- ➢ **Information Superiority**

- ➢ **Network Superiority**

- ➢ **Decision Superiority**

Two GIG Emerging Information Technologies

➢ **Information Superiority – Information Assurance Global Information Grid Enterprise Services (GES)**

➢ **Network Superiority – Network Enabled Net-Centric Operations and Warfare Reference Model (NCOW RM)**

➢ **NCR => Information Superiority + Network Superiority**

Global Information Grid Enterprise Services (GES)

➢ **Support Joint Functional Concept/Joint Operational Concept**

➢ **Pertains to the warfighter, business, and intelligence domains and associated COI**
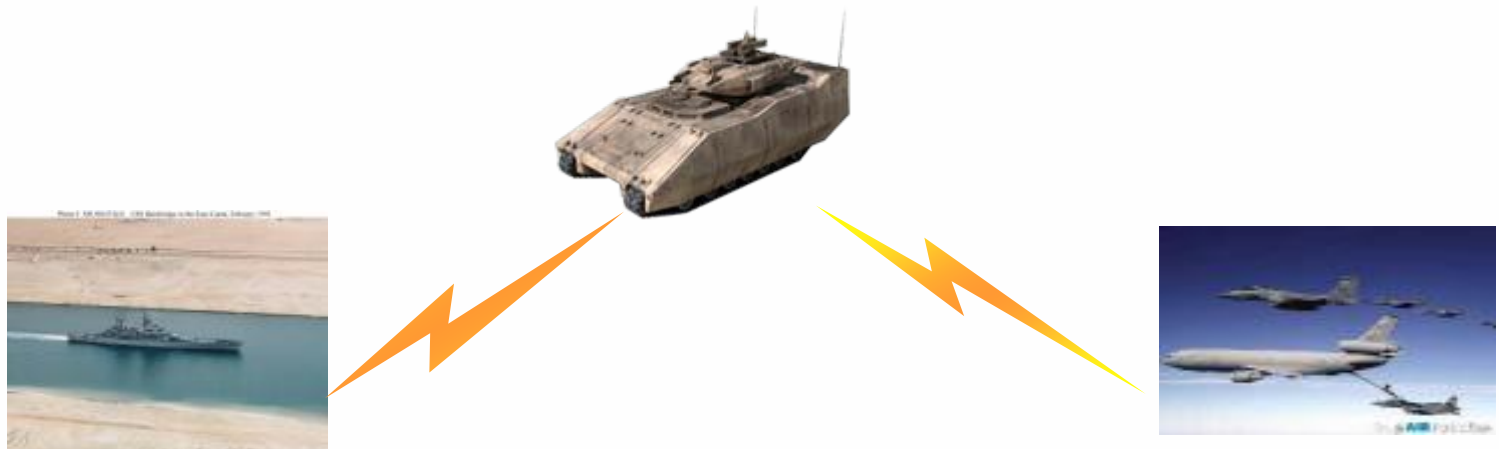
Information Superiority
GIG Enterprise Services (GES)

➢ **Warfighter Applications**

➢ **Business Applications**

➢ **Intelligence Information Services**

➢ **Communities Of Interest (COI)**

➢ **Cross Organization Services**

➢ **Joint Force/Allied Force Operational Infrastructure**

➔**Data**

↳ **Information**

↳ **Knowledge**

↳ **Decisive Decision**

↳ **Precise Action**

CECOM ——— PEO·C3T ——— PEO·IEW&S ——— PEO·EIS ——— CERDEC
COMMUNICATIONS ELECTRONICS LIFECYCLE MANAGEMENT COMMAND

Net-Centric Business

➢ **Installation & Environment**

– **Acquisition/Logistics -- Plan/Manage/Maintain**

➢ **Human Resources Plan/Manage**

– **Strategic Planning & Budgeting**

– **Accounting & Finance**

Net-Centric Warfighter

- ➢ **Force Applications**

- ➢ **Force Health Protection**

- ➢ **Command & Control**

- ➢ **Commander/Soldier Support**

- ➢ **Battlespace Situational Awareness**

- ➢ **Warfighter & Systems Interface**

Net-Centric Intelligence Information

- ➢ **Domain**

- ➢ **Cross Domain**

- ➢ **COI**

- ➢ **Joint Force and Multi-National Partners**

Net-Centric Acquisition/Logistics

- ➢ **Supply Distribution and Asset Visibility**

- ➢ **Property Accountability**

- ➢ **Materiel Management**

- ➢ **Maintenance Management**

Net-Centric Data Readiness

➢ **Data Accessibility**

➢ **Data Visibility**

➢ **Data Management**

➢ **Data Quality**

➢ **Data Interoperability**

➢ **Data Essential – Meet User's Need**

Net-Centric Information Readiness

- ➤ **Reach Capability -- Timely**

- ➤ **Richness Capability – Meet User's unique Needs**

- ➤ **Agility Capability – Collaboration**

- ➤ **Information Assurance**

Net-Centric Enterprise Systems Readiness

- ➢ **A System – A Single System level (Vertical) Readiness**

- ➢ **Family of Systems – Multi-Systems Level (Horizontal) Readiness**

- ➢ **Knowledge Sharing -- Consolidated Awareness**

- ➢ **Joint/Allied Forces– Cross Levels and Multi-National Levels**

Net-Centric Network Readiness Compliance with GIG

➢ **Enable Seamless Network – Robust, scalable, reliable Network**

➢ **Support and connect the interoperable heterogeneous networks environment**

➢ **Effectively and efficiently transfer information between users (end-to-end systems) in both tempo and space domains – leverage the functions of Network Management**

➢ **Ensure the Quality of Network Services -- Quality of Services (QoS)**

➢ **Host all joined systems and provide the common operating and processing environment**

FCS for Net-Centric Readiness
Information Superiority

- ➢ **Provide functionalities: Warfighter-Machine Interface Services, Logistics Decision Support Services, Platform and Soldiers Support Services, Battle Command (BC) Mission Planning and Preparation, Situation Understanding, BC Mission Execution**

- ➢ **Provide Intelligence, Reconnaissance and Surveillance (ISR) functionalities for a distributed and networked array of multi-spectral sensors – Protect, Detect, React, Recover**

- ➢ **Collect the data from the various distributed ISR and other sensor assets – Sensor Data Management**

FCS Compliance with NCOW RM
Network-Centric Superiority

➢ **Provide System of Systems Common Operating Environment to support multiple critical mission services and applications**

➢ **Enable the network to connect all supported family systems to the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)**

➢ **Provide functionalities to support the integrated network management, information assurance and dissemination management among sensors, processors and warfighters**

Information Superiority
Challenges/Shortfalls

➢ **Data ACID properties -- Atomicity, Consistency, Isolation, Durability**

➢ **Information Integrity**

➢ **Knowledge Assurance**

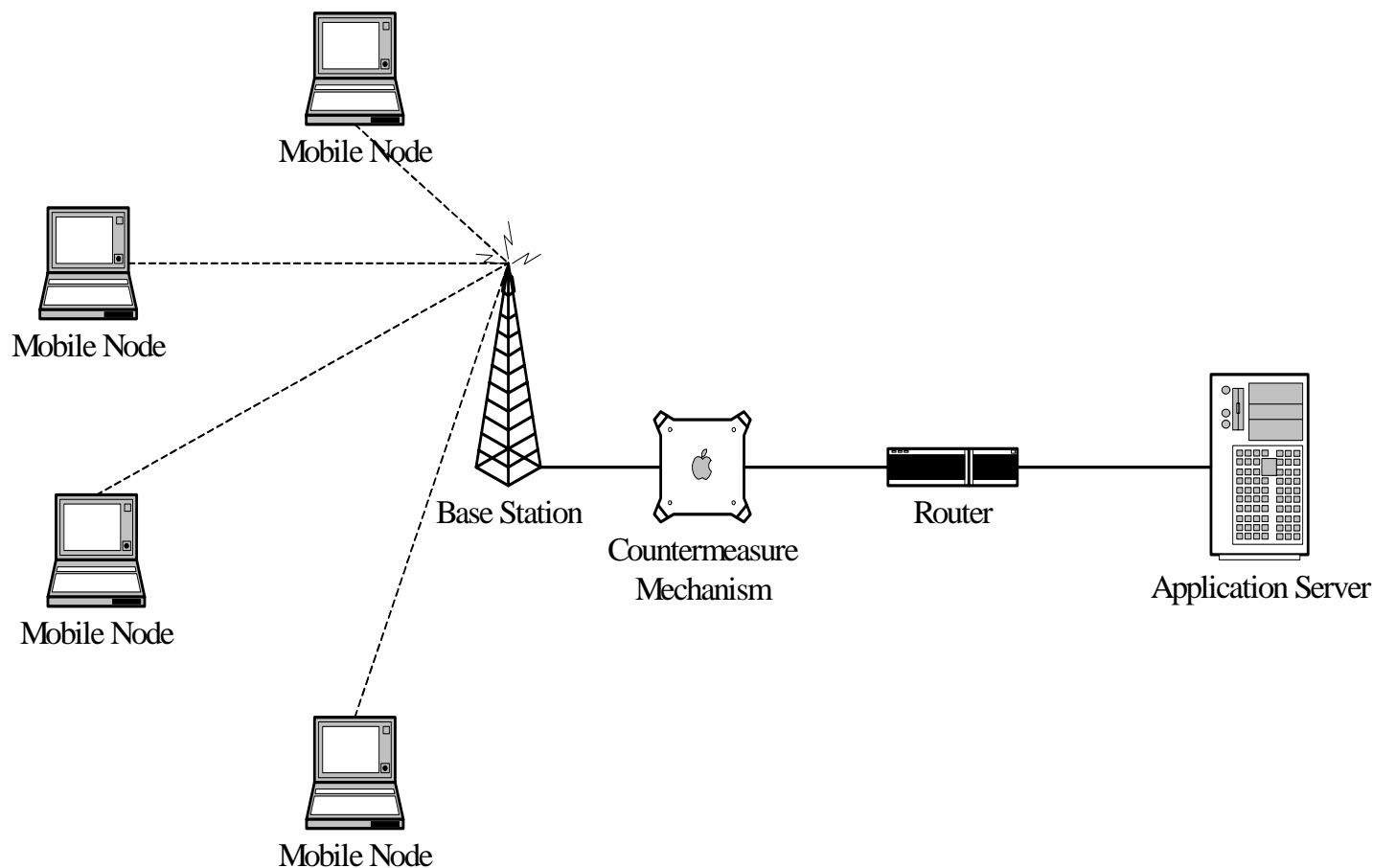➢ **Adversary/Terrorist Attack**

Network Superiority
Challenges/Shortfalls

➢ **Open/Heterogeneous Network Environment – interoperability**

➢ **Neither emerging DoD technology clearly addresses network security issues -- Guidance**

➢ **Unanticipated/Unpredictable Adversary Attack**

➢ **Cross Domain Constraints – Policies, Doctrine, Standards**

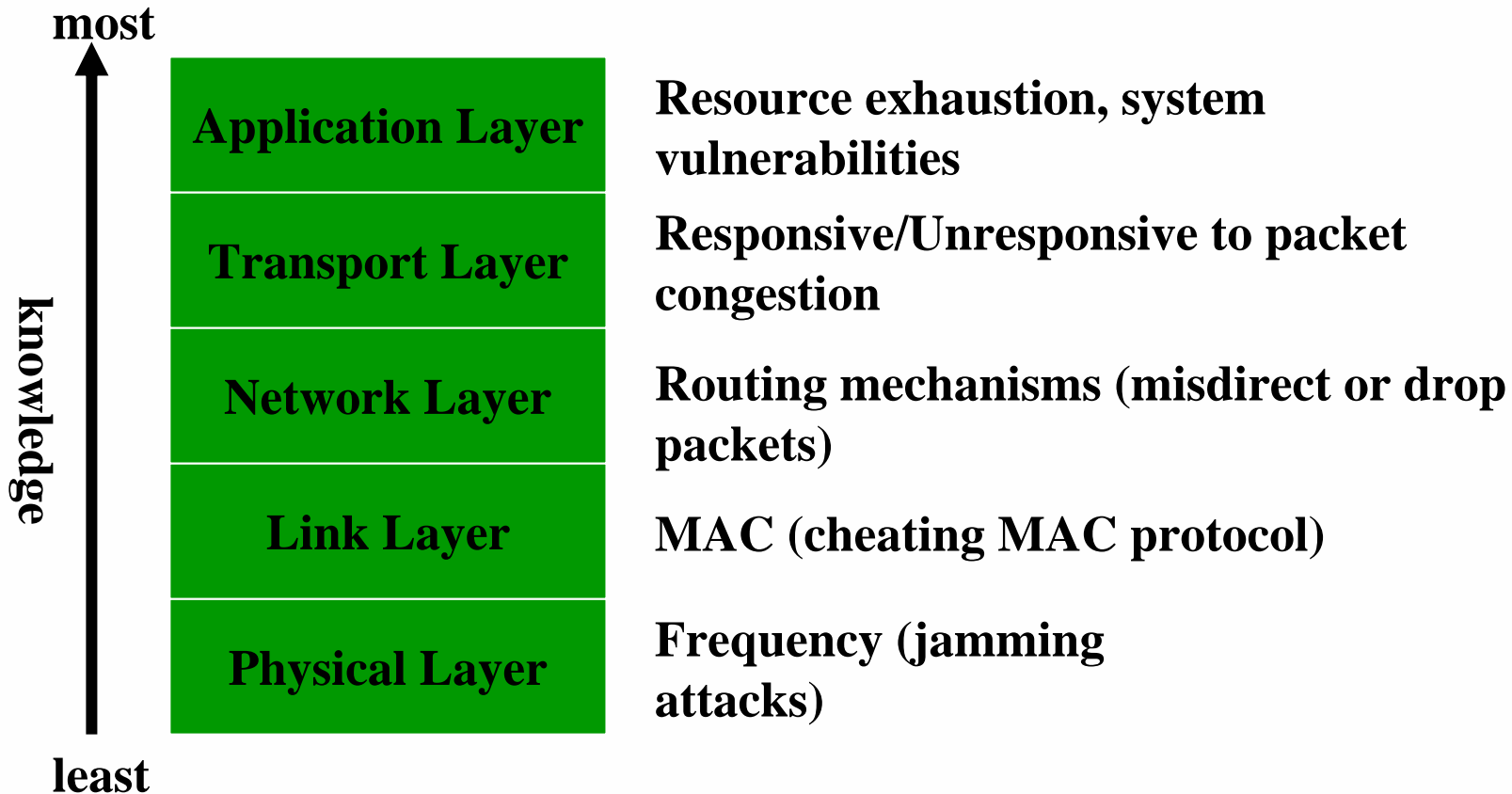➢ **Improvisational Organization/Network**
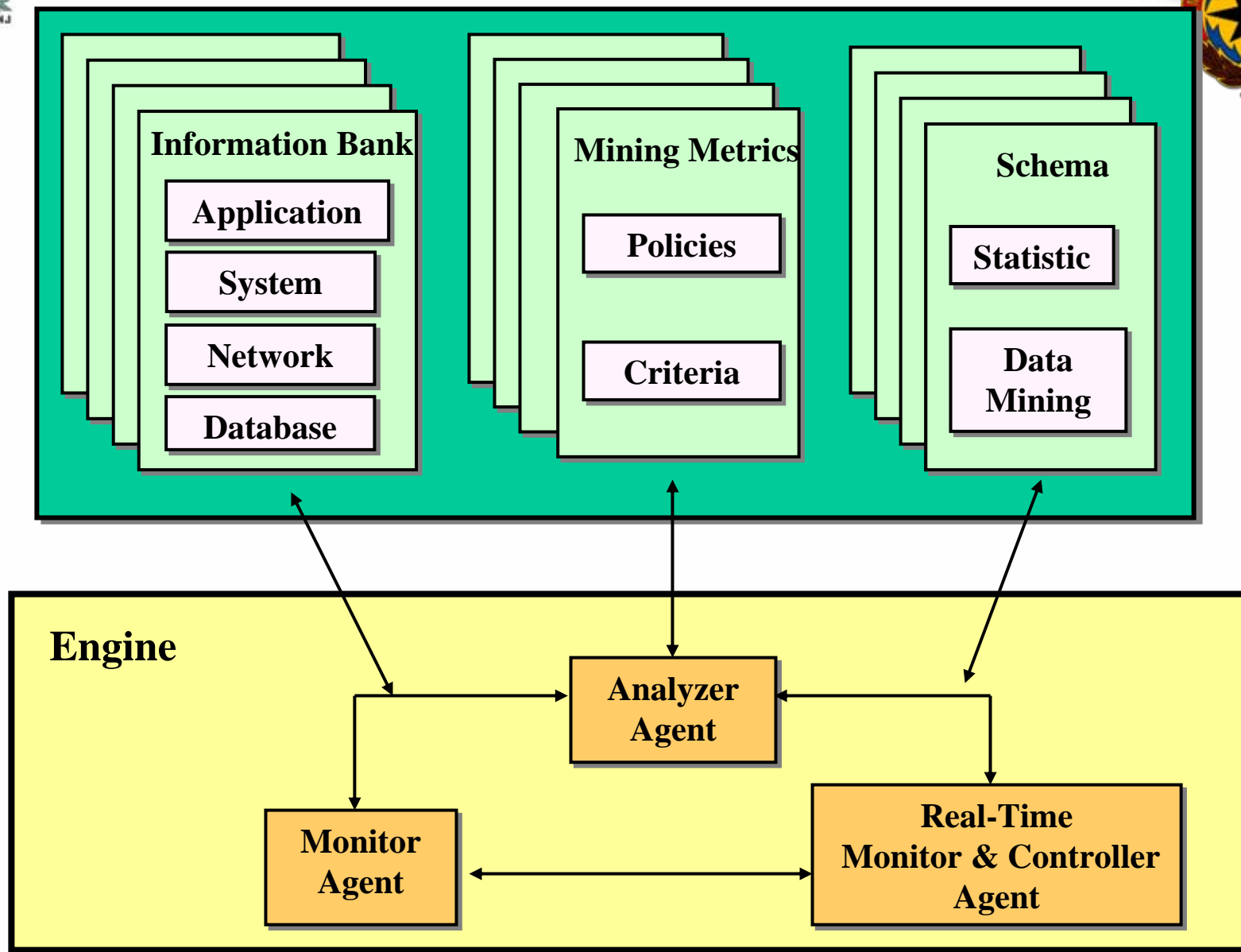
Countermeasures for Supporting
NCR / RAM-T

➢ Knowing the Challenges, Shortfalls, and Risk/Vulnerability Issues

➢ Enhance the data flow and network bandwidth utilization

➢ Monitor, Analyze, Control, Manage, and Model the Application Layer – Middle-ware

➢ Monitor, Analyze, Control, Manage , and Model network traffic behaviors – Multi-Layers

Points of Control and Observation

Mobile Node

Mobile Node

Mobile Node

Mobile Node

Base Station

Countermeasure Mechanism

Router

Application Server

Multi-Layers Control Mechanisms

most

knowledge

least

Layer	Mechanism
Application Layer	**Resource exhaustion, system vulnerabilities**
Transport Layer	**Responsive/Unresponsive to packet congestion**
Network Layer	**Routing mechanisms (misdirect or drop packets)**
Link Layer	**MAC (cheating MAC protocol)**
Physical Layer	**Frequency (jamming attacks)**

Information Bank

- Application
- System
- Network
- Database

Mining Metrics

- Policies
- Criteria

Schema

- Statistic
- Data Mining

Engine

- Analyzer Agent
- Monitor Agent
- Real-Time Monitor & Controller Agent

Countermeasures – Case Study
Secure the Sensor Network

➢ **Identify the challenges of distributed sensor networks:**

- **Scalability**
- **Connectivity**
- **Storage**
- **Resilience**
- **Energy**

➢ **Survey the existing solutions: Key Management Key Distribution Mechanisms**

Key Management Schemes

- ➢ **Mission Critical Sensor Nodes require efficient key distribution and management mechanisms**

- ➢ **Evaluate deterministic, probabilistic, and hybrid type of pre-distribution key algorithms for:**

  - **Pair-wise (unicast)**
  - **Group-wise (multicast)**
  - **Network-wise (broadcast)**

Single Master Key Based Scheme

➢ Pre-loads one single network-wide shared key for all nodes, such as Tiny SEC

➢ Pros:
- Good performance for storage
- Good performance for scalability
- Good performance for key connectivity, processing, and communication

➢ Cons:
- Bad performance for resilience

All Pair-Wise Keys Scheme

➢ Every node shares a unique key with every other node

➢ Pros:
  • Good performance for resilkience

➢ Cons:
  • Bad performance for storage; n(n-1)/2 keys for the entire network

Random Pair-Wise Key Scheme

➤ Basic scheme: sensor nodes share a probabilistic subset of keys selected from a large key pool

➤ Improved scheme: Pair-Wise key paired with unique ID or share crypto parameters from key space

➤ Pros:
- Good performance for resilience

➤ Cons:
- Bad performance for processing and communication
- Bad performance for scalability and key connectivity
- Bad performance for resilience if storage is not enough
-

Group-Based Key Scheme

➢ Sensor nodes within group share unique pair-wise in-group keys and share inter-group keys with neighboring nodes from different group

➢ Pros:
  • Good performance for resilience
  • Good performance for scalability and key connectivity

➢ Cons:
  • Bad performance for processing and communication
  • Bad performance for scalability, key connectivity, and resilience if the storage is not available

Trusted Base Station Scheme

➢ A trusted and secure base station is an arbiter to provide link keys to nodes. Authentication of nodes is done by the base station, such as SPINS

➢ Pros:
   - Good performance for storage
   - Good performance for resilience
   - Good performance for revocation of nodes

➢ Cons:
   - Bad performance for single point of failure

Data Memory available for Security in CrossBow
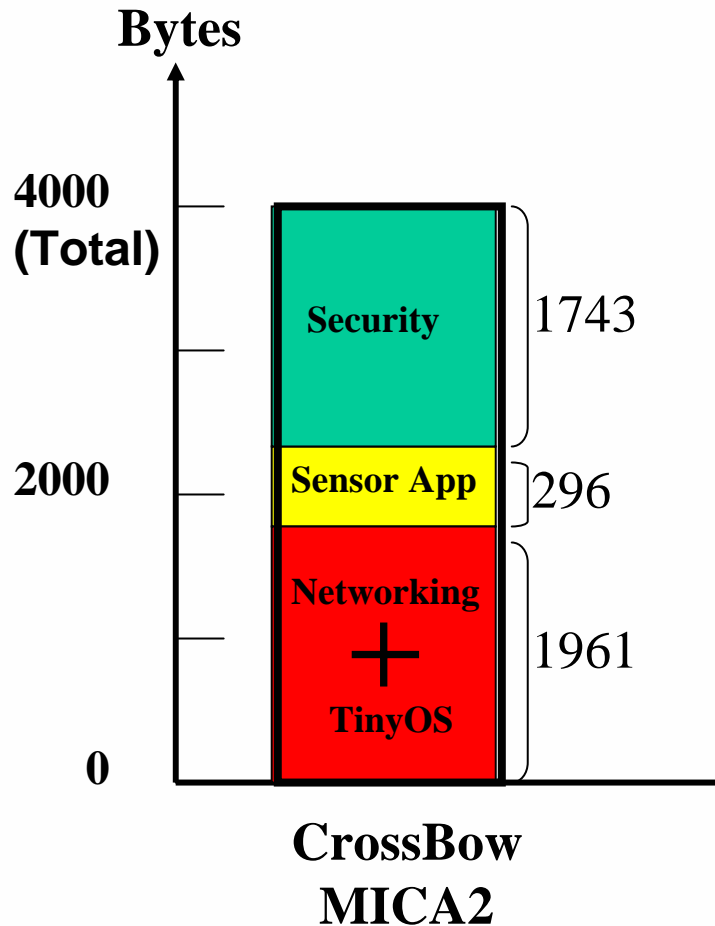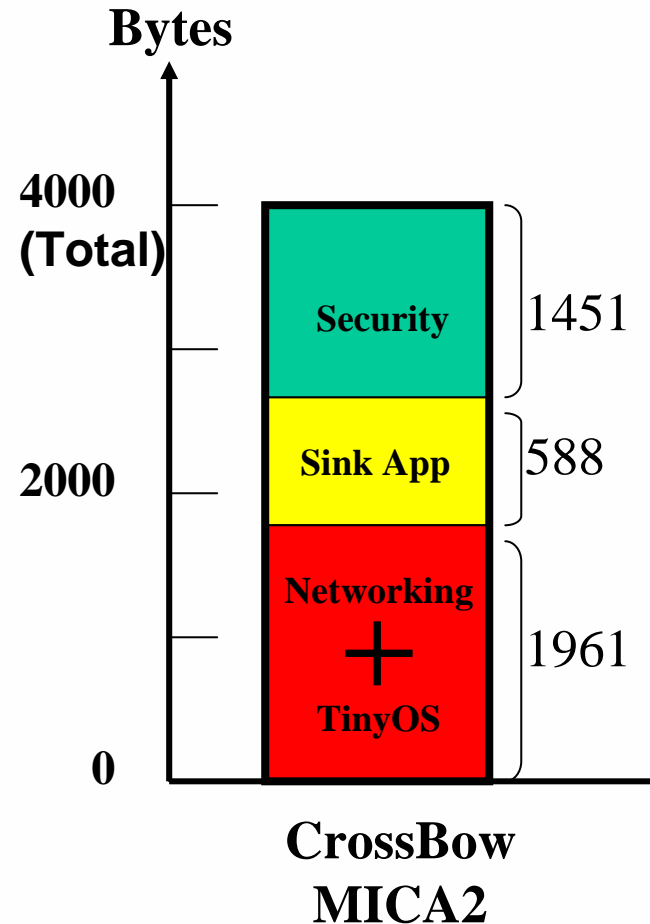
Conclusion – Winning is ours

➢ **GIG provides the road to Net-Centric Readiness :**
- • **GES Provides the road to ensure Information Superiority**
- • **NCOW RM Provides the road to ensure the robust, available, and interoperable Network Superiority**

➢ **Information and network assurance bring accurate information to the battlefield commanders to enhance decision-making and action**

➢ **FCS proves the concept of Net-Centric Readiness**

➢ **Challenges of both information and network superiority require further embracing of the research efforts**

➢ **Challenges of secure wireless sensor networks will be the subject of future research.**

Acronyms

BC	Battle Command
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance
COI	Communities of Interests
FCS	Future Combat System
GES	Global Information Grid Enterprise Service
GIG	Global Information Grid
ISR	Intelligence, Surveillance, and Reconnaissance
NCOW RM	Net-Centric Operation and Warfare Reference Model
NCR	Net-Centric Readiness